Media Protection Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Reviewed Date – 05/17/2024

1. Purpose

Establish the enterprise policy for managing risks from media access, media storage, media transport, and media protection through the establishment of an effective media protection program.

2. Authority

DC Official Code § 1-1401 et seq., provides the Office of the Chief Technology Officer (OCTO) with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District of Columbia Government (District). This document can be found at: https://code.dccouncil.gov/us/dc/council/code/sections/1-1402.

3. Applicability

This policy applies to all District Workforce members performing official functions on behalf of the District, or any District agency/District/entity who receive enterprise services from OCTO. In addition, this policy applies to any providers and third-party entities with access to District information, networks, and applications.

4. Policy

District agencies must develop or adhere to a strategy which demonstrates compliance with this policy and its related standards. The following outlines the requirements for this policy. OCTO will review, update, and disseminate this policy annually at a minimum, to ensure accuracy, clarity, and completeness. The District's agencies must develop and review or update annually and after changes to the policy, a procedure in support of this policy with the following requirements.

4.1. Media Access

District agencies must restrict access to digital and non-digital media to authorized personnel using physical access controls and safeguards.

4.2. Media Marking

District agencies must:

4.2.1. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

4.2.2. Exempt District agencies' confidential and sensitive information from marking if the media remains within designated agency's workspaces, e.g. agency HQ and Data Centers.

4.3. Media Storage

District agencies must:

4.3.1. Physically control and securely store District information systems and backup media within securely controlled areas and/or in a protective container with oversight by authorized personnel.

4.3.2. Protect information system media until it is destroyed or sanitized.

4.4. Media Sanitization

District agencies must:

4.4.1. Sanitize all information system media (both digital and non-digital) using approved equipment, techniques, and procedures prior to disposal, release from organizational control, or release for external reuse.

4.4.2. Employ appropriate sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

4.5. Media Use

District agencies must:

4.5.1. Restrict the use of removable media on information systems unless required for system maintenance or other procedure, e.g., such as backing up or preparing data for delivery to external users.

4.5.2. Encrypt all removable media used to store all District sensitive information.

5. Exemption

Exceptions to this policy shall be requested in writing to the Agency's CIO and the request will be escalated to the Chief Information Security Officer (CISO) for approval.

6. Definitions

The definition of the terms used in this document can be found in the *Policy Definitions website*.